



Annual Security Training

Security Message

The protection of government assets, people and property, both **classified** and official but unclassified, **is the responsibility of each and every member of the Department of Defense (DoD), regardless of how it was obtained or what form it takes.** Our vigilance is imperative in the protection of this information. Anyone with access to these resources has an obligation to protect it.

The very nature of our jobs dictates we lead the way in sound security practices. Anything less is simply not acceptable.

E Pluribus Unum



Annual Security Training

Fort Drum and the 10th Mountain Division (LI)

By Pete Hansen

Security and Intelligence Division

Directorate of Plans, Training, Mobilization and Security

peter.hansen@us.army.mil

(315) 772-7465 DSN 772-7465

Slides available on Fort Drum's MountaiNet website: <https://mountainet.drum.army.mil/>

WHAT'S HOT

We are at Force Protection Condition Alpha (FPCON A)! If you have questions as to actions you need to take, contact your Security Officer. [Click Here](#) for more information.

To assess the FY 07 Threat Assessment. [Click Here](#).

Homeland Security Advisory System Threat Level for the Aviation Sector, including all domestic and international flights, is **ORANGE-HIGH**. The U.S. Threat Level is **YELLOW-ELEVATED** for all other sectors and areas in U.S. As of 3 Nov 06.

DOCUMENT LINKS

FOLDERS

-  Force Protection
-  Foreign Disclosure
-  Industrial Security
-  Information Security
-  Installation Security News
-  Operation Security
-  Personnel Security

FILES

- ▶ Area of Responsibility Templates.htm
- ▶ Installation Security News.htm
- ▶ SecurityResponsibilities.pdf
- ▶ SID Mission and Hours of Operation.htm
- ▶ Training.htm
- ▶ Travel Warnings.htm

NEWS & INFORMATION

Are you planning to Travel Oversea (including Canada)??? If so, DoD and DA (AR 525-13) requires all Soldiers to obtain mandatory Antiterrorism / Force Protection (AT/FP) Level I Awareness Training and country updates (Area of Responsibility (AOR) briefings) prior to traveling. When traveling on orders, family members, age 14 years or older, and civilians will receive similar training prior to their traveling outside the United States, its territories and possessions. DoD-employed contractors are encouraged to attend AT/FP Level 1 and AOR briefings.

Changes in Entry Requirements.

□ ALL persons, including U.S. citizens, traveling by air between the United States and Canada, Mexico, Central and South America, the Caribbean, and Bermuda will be required to present a valid passport, Air NEXUS card, or U.S. Coast Guard Merchant Mariner Document, or an Alien Registration Card, Form I-551.

□ As early as 1 Jan 08, ALL persons, including U.S. citizens, traveling between the U.S. and Canada, Mexico, Central and South America, the Caribbean, and Bermuda by land or sea (including ferries), may be required to present a valid passport or other documents as determined by the Department of Homeland Security. While recent legislative changes permit a later deadline, the Departments of State and Homeland Security are working to meet all requirements as soon as possible. Ample advance notice will be provided to enable the public to obtain passports or passport cards for land/sea entries.



Soldier & Civilians' Guide to Security! To access, click on the Security Icon to the left.



Annual Security Training is now available. To access, click on the lock Icon to the left.



Interactive Customer Evaluation (ICE) - Fort Drum's on-line customer comment card system. This is your opportunity to help improve Fort Drum services by Clicking ICE





Annual Security Training

Objectives

- Why You Are Here (security manager duties)
- Required Training (tailored and records)
- Original and Derivative Classification (challenging)
- Marking Classified Material
- Controlling Access (most difficult)
- Storage, Reproduction, Transmission, Transportation, Dissemination and Destruction of Classified
- Procedures for Securing Electronic Classified Information and Automation
- Inspections
- Threat
- Security Violations and Incidences (penalties)



Annual Security Training

Security Manager Duties



- Advise and Represent the Commander.
- Manage and Execute Unit Security Program. *
- Develop Unit Security Policy and Procedures.
- Manage Unit Security Education Program.
- Write / Interpret Classification Guides.
- Help Solve Classification Problems.
- Develop Procedures and Manage Access: Ensure All Personnel with Access to Classified Information are Properly Cleared.
- Safeguard and Protect Classified: Responsible for Classified Material Accountability. Consider a Classified Document Custodian for Secret: required for Top Secret.
- Review Classified Holdings / Reduce Unneeded Material.
- Conduct Inspections and Spot Checks.
- Enforce Regulations and Policies.
- Maintain Unit Security Clearance Access Roster.
- Emergency Evacuation & Destruction Plan.

* Starts with In and Out-processing Your Units' Personnel.



Annual Security Training

Why are we here?

■ AR 380-5, Information Security Program:

- All Personnel: Initial Training within 60 days of Arrival.* **Unit responsibility**
- All Personnel that have Access to Classified Material: Unique Security Training Tailored to their Specific Role, Duties and Access. **Unit responsibility**
- Annual Refresher Training
- Security Manager Training: IAW para 9-12.* **Also - SID as requested SID provides quarterly**

■ AR 380-67, Personnel Security: Initial and Annual.* **SID as requested**

■ AR 25-2, Information Assurance: Initial and Refresher IA Awareness training.

DOIM provides several times a year

■ AR 381-12, Subversion and Espionage Directed Against the US Army (SAEDA): Annual training. **DPTMS / 902nd provides monthly**

■ AR 530-1, OPSEC: Orientation within 90 days of arrival and annually thereafter.

■ AR 525-13, AT: Annual training, and Travel briefs within two-months of travel, including Canada. **DPTMS provides monthly**

***NOTE: Requirement Satisfied by this Training**



Annual Security Training

Three Categories of CLASSIFIED Information:

- **TOP SECRET:** Exceptionally Grave Damage
- **SECRET:** Serious Damage to National Security
- **CONFIDENTIAL:** Identifiable Damage

Some categories of SENSITIVE Information:

- For Official Use Only (FOUO)
- Sensitive But Unclassified (SBU)
- Privacy Act Information
- Law Enforcement Sensitive (LES)
- Controlled Unclassified Information (CUI)





Annual Security Training

How is information classified?



- Original Classification
- Derivative Classification



Annual Security Training

Original Classification Authority (OCA)

- Specified by E.O. 12958 and DoD 5200.1-R – Only about 1,200 DoD positions have classification authority.
- As it relates to Fort Drum:
 - Top Secret: Commanding General, U. S. Army Forces Command
 - Secret and Below:
 - FORSCOM DCG, DCofS G-2 and DCofS G-3
 - CG, 10th Mountain Division (Light)
- Must be trained in the Original Classification Process



Annual Security Training

Original Classification Process

- Determine the current classification status
- Determine if official government information.
- Determine if in an authorized category. *
- Determine if prohibited intent or type. **
- Determine likelihood of damage to national security and be able to identify or describe the damage.
- Weigh advantages and disadvantages.
- Determine the level of classification.
- Make a decision about the duration of classification.
- Communicate the decision (Classification Guides).



Annual Security Training

Authorized Classification Categories

As Specified by EO 12958 Section 1.4

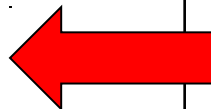
- Military plans, weapons or operations – 1.4(a).
- Foreign government information – 1.4(b).
- Intelligence activities, intelligence sources or methods, or cryptology – 1.4(c).
- Foreign relations of foreign activities of the US, including confidential sources – 1.4(d).
- Scientific, technology or economic matters relating to national security, which includes defense against transnational terrorism – 1.4(e).
- US government programs for safeguarding nuclear materials or facilities.
- Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security, which includes defense against transitional terrorism – 1.4(g).
- Weapons of mass destruction – 1.4(h).




Annual Security Training

Derivative Classification

- Incorporating, paraphrasing, restating or generating in a new form, information that is already classified
- Written authority is not needed



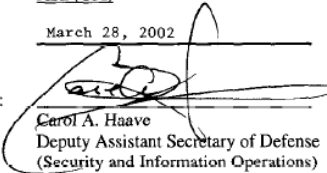
 OASD(C3I)/S&IO


SECURITY CLASSIFICATION GUIDANCE

TITLE: Operation ENDURING FREEDOM and Operation NOBLE EAGLE

ISSUED BY: ASD(C3I)

DATE: March 28, 2002

APPROVED BY: 
Carol A. Haave
Deputy Assistant Secretary of Defense
(Security and Information Operations)


John P. Stenbit, Senior Agency Official
Assistant Secretary of Defense
Command, Control, Communications and Intelligence

Local reproduction is authorized. Distribution limited to US Government Agencies and their contractors. Other requests for this document shall be referred to OPR.

This document contains information exempt from mandatory disclosure under the Freedom of Information Act (FOIA). Exemption 2 applies.

Destroy by any method that will prevent disclosure of contents or reconstruction of the document.



Annual Security Training

Derivative Classification - Cont.

| | | | | |
|---|--------------|------------|---------------|------------|
| 1.4 Specific details of allied country participation or support of Operation ENDURING FREEDOM that have not been published which would reveal information | SECRET | 1.5b, 1.5d | X-5, X-6, X-8 | See Note 3 |
| 1.5 General geographic location of units deployed in Operation ENDURING FREEDOM belonging to knowledge. | CONFIDENTIAL | 1.5a, 1.5b | X-5, X-6, X-8 | |

(TRAINING EXAMPLE ONLY)



Annual Security Training

SECRET

Derivative Classification - Cont. Proportional Marking: (U)

1. (FOUO) SPECIFIC FORCE PROTECTION MEASURES - CLASSIFIED SECRET.
2. (FOUO) READINESS DATA - CLASSIFIED SECRET.
3. (S) SPECIFIC VULNERABILITIES TO OPERATIONS, EQUIPMENT OR PERSONNEL RELATED TO SIGNIFICANT TROOP MOVEMENTS - CLASSIFIED CONFIDENTIAL (UNLESS CLASSIFIED HIGHER BASED ON OTHER SECURITY CLASSIFICATION GUIDANCE).

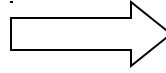
SECRET

(TRAINING EXAMPLE ONLY)



Annual Security Training

Your
Source Document
Document
Received



SECRET

Memo: Training Only
(U)

1. (C) This paragraph is confidential
2. (S) This paragraph is Secret

SECRET

(TRAINING EXAMPLE ONLY)

SECRET

Memo: Derivatively Classifying
From a Source Document (U)

1. (U) This paragraph is unclassified
2. (U) This paragraph is unclassified
3. (S) This paragraph contains secret information paraphrased from the source document received

SECRET

(TRAINING EXAMPLE ONLY)



Annual Security Training

Associated Markings (Title Page):

SECRET

SPECIFIC FORCE PROTECTION MEASURES (U)

25 Apr 06

Defense Interoperability Agency

4444 Dove St, Springfield, Virginia 22150

Derived from: Multiple Sources

Declassified on: 29 Jun 2031*(most restrictive)*

Date of source: 29 Jun 06 *(most recent)*

Sources: Laser Widget Test, DIVA, 14 Mar 01

Laser Demo, DIVA, 29 Jun 06

SECRET

(TRAINING EXAMPLE ONLY)

E Pluribus Unum



Annual Security Training

For Official Use Only (FOUO)

What Information You Can Mark as FOUO - AR 25-55

- Internal Personnel Rules and Practices, and Deliberative Memos. Category #2
- As Exempt by Statute (e.g., NSA & Patent Information, Restricted Data and Formally Restricted Data, Nuclear Material, Communication Intelligence and Intelligence #3 Sources and Methods, Certain Technical Data, Medical Quality Data). #4
- Trade Secrets, or Commercial or Financial Information. #5
- Intra and Interagency Internal Advice, Recommendations and Evaluations; Budget information; Attorney-client Information. #6
- Personal, Medical and Privacy Information; Directories of Deployed Units; Names of Personnel Assigned to Sensitive Units; Information to Protect Surviving Family Members. #7
- Law Enforcement Records or Proceedings, Investigative Techniques, Individual Trial Information, and Confidential Sources. Information that could put Lives at Risk. #8
- NOTE: Other laws, statutes, regulations may specify that specific information may be marked FOUO. Geological and Geophysical Information. #9





Annual Security Training

Questions?

FORT DRUM'S MOUNTAINET WEBSITE:
<https://mountainet.drum.army.mil/>

&

DEFENSE SECURITY SERVICE (DSS) ACADEMY MISSION
www.dss.mil

The DSS Academy provides security education and training to Department of Defense (DoD) security program professionals, DoD contractors, employees of other Federal agencies and selected foreign governments. Its professional staff of instructors, technology professionals, and education support personnel combine expertise to create, collaborate and facilitate delivery of quality education and training across the security disciplines.

General Security
Information Security
Operations Security
Physical Security

Industrial Security
Information Systems Security
Personnel Security
Special Access Programs



Annual Security Training

Protecting Classified Information

"We have an obligation to protect military, operational security, intelligence sources and methods, and sensitive law enforcement investigations."



President George W. Bush, Memo Directed FBI, CIA, State, Treasury and Defense to Release Classified Information only to Four Major Congress Leaders and Intelligence Committee Members, October 5, 2001



Annual Security Training

Proper Security Practices

- ✓ Protecting Classified
- ✓ Transmission
- ✓ Destruction
- ✓ Reporting Requirements



Annual Security Training

Protecting Classified at Work

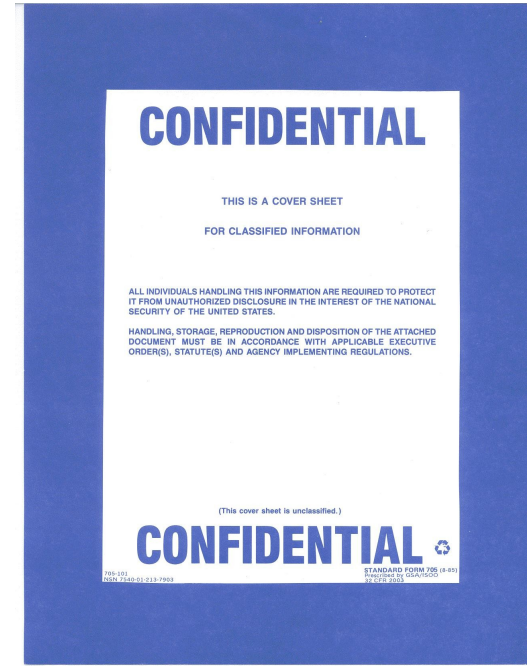
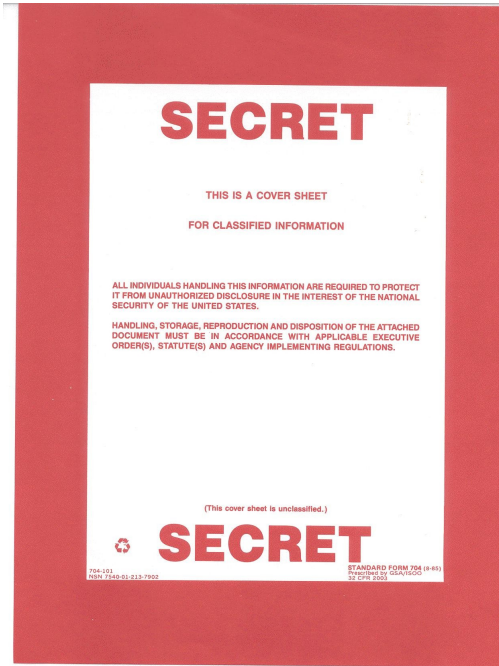
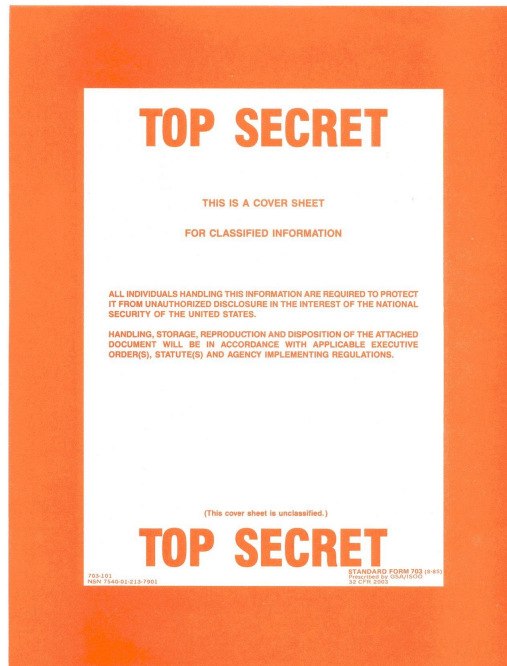
Properly Mark Classified Information

- Titles and Paragraphs marked
- Document marked at highest level of classified information contained in it
- Cover, front and back, top and bottom
- Classified by line
- Declassification instructions



Annual Security Training

Protecting Classified at Work



Use cover sheets!



Annual Security Training

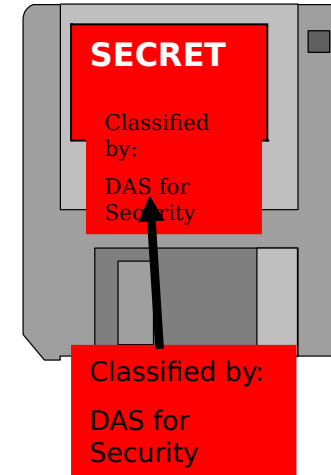
Protecting Classified at Work

Mark Classified Information Computer Media



- Affix labels with highest classification contained within
- Include as much other information as possible, i.e. authority and declassification instructions
- DVD/CD: Mark the DVD/CD and case.
- USB Drives: Mark the device.

Don't place classified media into unclassified automation: causes a compromise!





Annual Security Training

Protecting Classified at Work

Classified information must be stored in a GSA-approved security container (safe) when not in use (**For source information:** <https://portal.navfac.navy.mil/go/locks>).

DO NOT STORE CLASSIFIED IN THE FOLLOWING:

- Filing Cabinets
- On Top of Safes
- Window Sills



Annual Security Training

Protecting Classified at Work

Safe Combinations

- Security container combinations are classified at the level of information in the safe
- Memorize combinations; never write them down (except on SF 700)
- Don't share with anyone who does not need to know
- Use SF 702 to record opened and closed by information
- Use opened closed magnetic signs

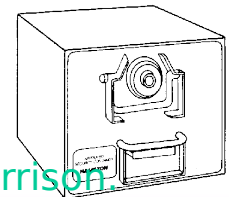


Who can you give the security container combination to?

When do you change the safe combination?

Is this container sufficient for Top Secret material?

Source: <https://portal.navfac.navy.mil/go/locks>



Field Safes: Are NOT authorized to store classified information in Garrison.

SECURITY CONTAINER CHECK SHEET

TO: [] THRU: []

SECURITY CONTAINER CHECK SHEET

FROM: [] THRU: []

SF702



Annual Security Training

Protecting Classified at Work

Minimum Storage Requirements

TOP SECRET:

- GSA approved container with supplemental controls (4 or 5-drawer)
 - Continuously Guarded Location
 - Guards checking GSA approved container every two hours
 - 15 minute IDS recall
 - Container within a container (security in depth)
- Vault with 15 minute IDS recall with security in depth
- GSA-approved modular vault with 15 minute IDS recall with security in depth
- Secure room with 15 minute IDS recall with security in depth

SECRET:

- Same as TS
- GSA approved container or vault without supplemental controls
- Secure room with supplemental controls



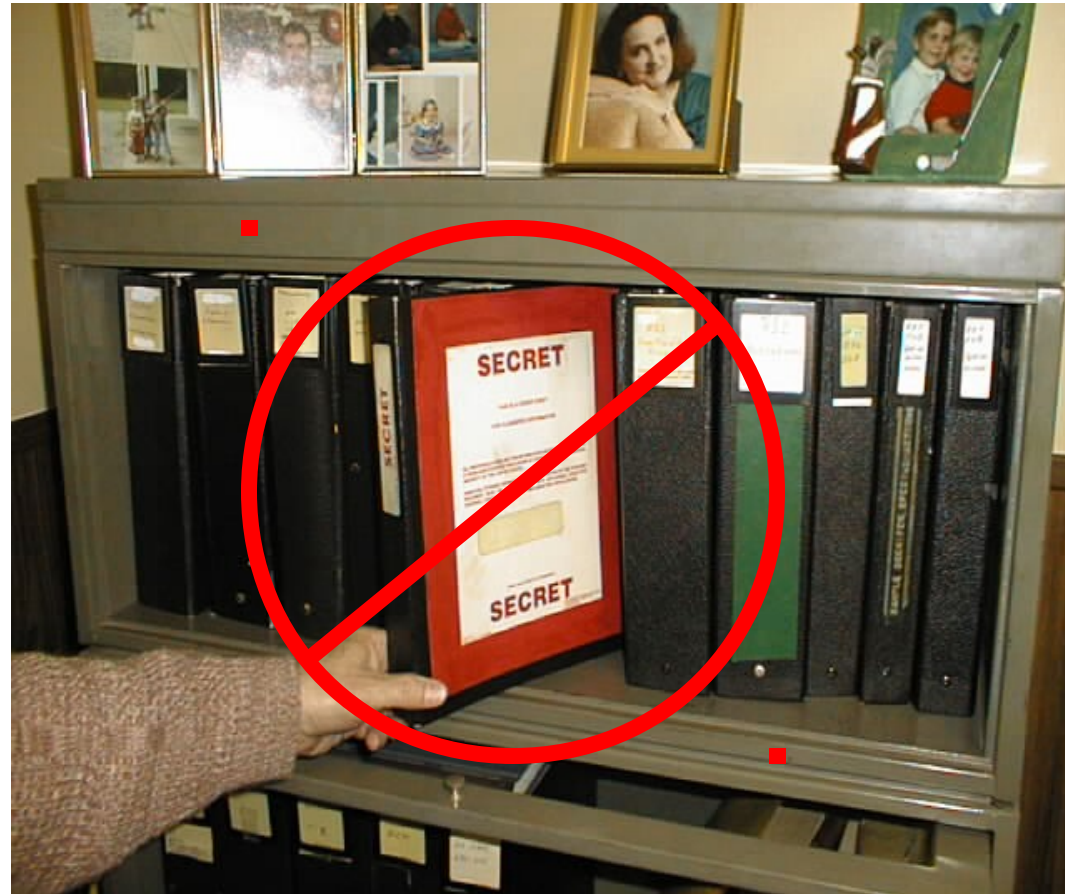
Annual Security Training STORAGE?





Annual Security Training

Uh-OH!





Annual Security Training

Security containers maybe marked with a number on the outside.

DO NOT mark classification level on the outside of the container

DO NOT place items on top of container





Annual Security Training

Protecting Classified at Work

Classified Briefings / Meetings

- Room / facility visually checked thoroughly and secured.
- Cleared guards at entrances, outside windows, etc.
- Access rosters.
- Disconnect telephones. Collect wireless devices.
- Cover windows.
- Check outside room / building for sound attenuation.
- Check for extra wiring, suspicious equipment, etc.
- Only use authorized audio / visual equipment, and automation.
- Secure classified waste.
- Any “notes” taken are classified working papers and must be secured.



Annual Security Training

Protecting Classified at Work Personnel Security

You must limit access to authorized persons by verifying:

- Identification and Need to Know (For Contractors - DD Form 254 and Expected)
- Personnel Security Clearance
 - Investigation as Recorded in JPAS
 - Access
- Ability to Protect (Trained and Courier Cards or Orders) ← KEY POINT.



Annual Security Training

Protecting Classified at Work

Personnel Security Clearances

- A Privilege; Not a Right
- Maybe revoked at any time (for cause)
- Investigation + CDR granted Access = Personnel Security Clearance
- Requires Investigation and Reinvestigations (5/10 /15 year marks)
- JPAS system of record (SF312 NDA date, CDR granted access, Unit ownership, personal data, and Investigation date).



Annual Security Training

Protecting Classified at Work

Personnel Security Investigation Process:

- Unit requesting memo to SID, with attached Medical and PMO checks
- SID will e-mail and provide memo through unit to individual granting access to e-QIP site (30-days to initiate & 90-days to finish). SID will also return all documentation.
- Individual inputs personal data, electronically validates it, and prints a reviewing copy.
- Security Manager reviews.
- Individual prints and sign signature pages, then electronically submits the e-QIP produced form.
- Security Manager provides all documentation to SID.
- SID will review. If needed, SID will request finger print cards and other documents. SID will submit the personnel security application.



Annual Security Training

Protecting Classified at Work

Foreign Disclosure:

- **Disclosure of Official DOD information to Foreign Governments, International Organizations, and Contacts with Foreign Representatives**
- **Personnel Exchange Program (PEP)**
 - Must have a Delegation of Disclosure Authorization Letter (DDL) Outlining Information allowed to be disclosed.
 - Foreign Disclosure Officer Ensures Compliance with Terms of the DDL.
 - PEP Officers are not Allowed Command Assignment Positions.
 - PEP Individuals May Not have Unsupervised Access to Automation (normally only visual / oral disclosure).
 - **PEP Individuals Can Not Obtain US Security Clearances,.**
 - PEP Individuals may not be given Security Responsibilities.



Annual Security Training

Protecting Classified at Work

Transmitting Classified (Voice)

- Always use Secure Telephone Equipment (STE) for classified calls (e.g., NSA approved cryptographic system).
- Use compatible facsimile machines cleared for classified use for quick and secure document transmission.
- Check windows and doors before classified conferences to ensure others can not hear or see what is going on. Control access with guards.
- Remove unauthorized wireless devices from area.

STU III – Dec 08 is the last time DoD will generate a STU III cryptographic variable. DoD will end STU III use Dec 09.



Annual Security Training

Protecting Classified at Work

Transmission (Hand-Carrying)

Secret and **Confidential** Only

- **On Post: DD Form 2501**
 - JPAS indicated access and investigation
 - Acknowledgement of Responsibilities
 - Only on Fort Drum
- **Off Post: Orders (CONUS & OCONUS)**
 - Double wrapping and addressing
 - Receiving and sending POC information
 - Inventory / receipt
 - Acknowledgement (CONUS or OCONUS)
- **Two-way Hand-carrying not Authorized**

NOTE: G-2 produces for 10th MTN DIV Units, and DPTMS, SID for Garrison / Tenants.

***Includes hard drives, pen drives, laptop computers and other electronic devices and components!!



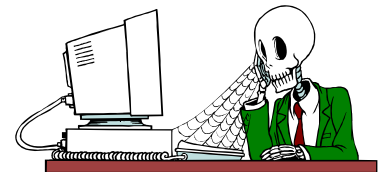
Annual Security Training

Protecting Classified at Work Automation

Transmitting Classified (Electronic)

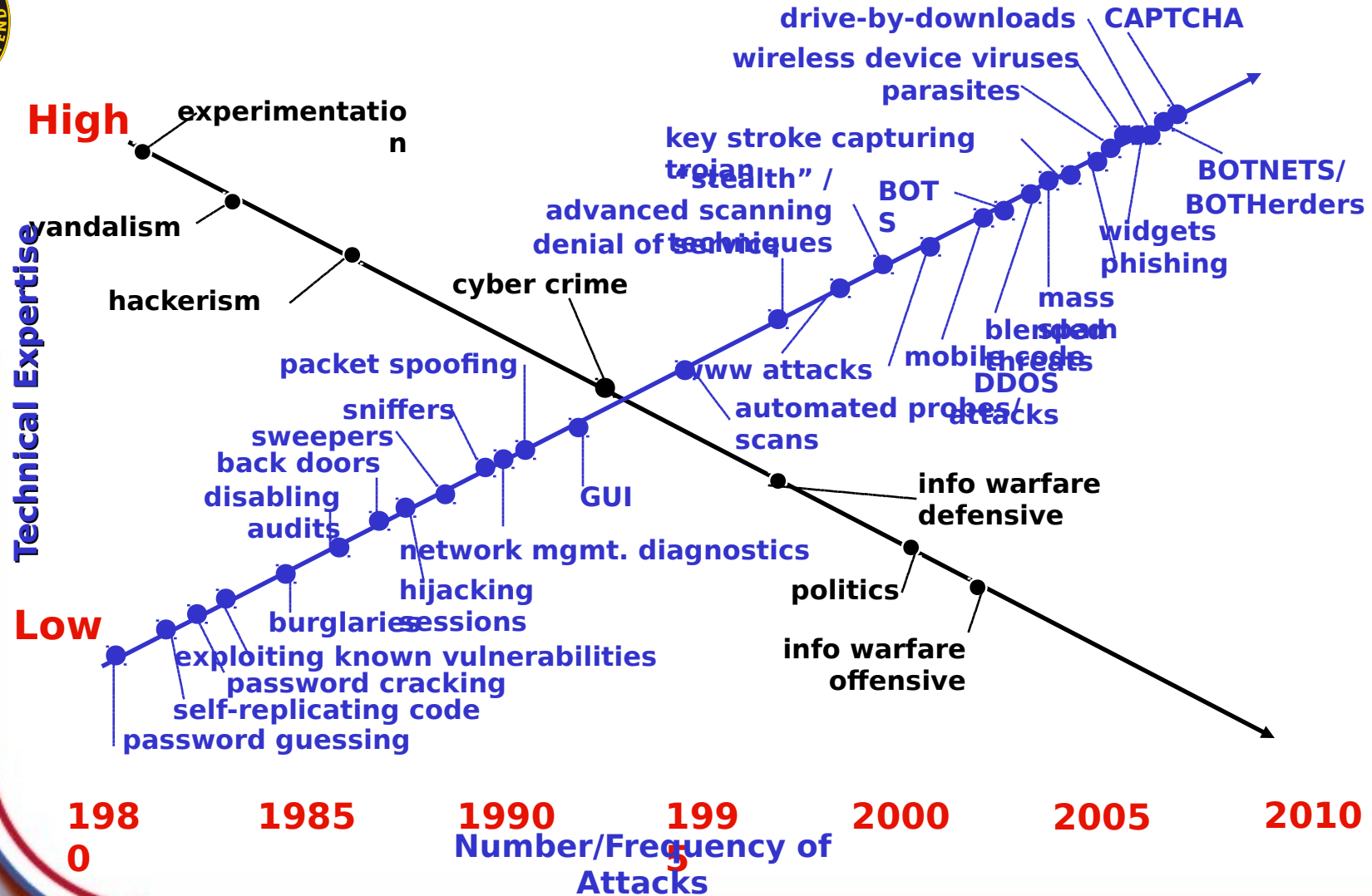
NO Unauthorized Use of Computers!

- Systems must be certified and accredited PRIOR to use (both Classified and Unclassified)
- Users must IT-Level III Trained
- All users must have a background investigation (including contractors)
- Protect classified automation and communications
 - Secure room
 - GSA approved containers
 - Secure classified components (e.g., removable HD, TACLANE & CIK or PDS)
- See your IMO or IASO, or DOIM for help





Annual Security Training





Annual Security Training

Protecting Classified at Work

Reproduction of Classified Documents (Photocopier)

- Use approved equipment only (G2 is the only agency that has classified copiers)!
- Cannot connect to unclassified networks.
- Cannot leave latent images (ghosting).
- Classified material cannot be visible to uncleared personnel.
- Cannot retain electronic data (e.g., embedded HD's, memory or other components).
- POSTED and authorized (FORSCOM Form 138-R).
- Unit SOP indicating sanitation procedures (jams and classified waste).
- There is a risk of leaving originals in / on reproduction equipment.
- If you have a cleared copier, you must add "Checked Copier" to your End of Day checks on your SF 701.



Annual Security Training





Annual Security Training

Protecting Classified at Work

Destruction

- Approved Cross-cut Shredding, including paper and Mylar film (Disintegrator) - G2
- Classified waste “burn bags.” (environmental issues)
- Electromagnetic destruction (HD's) - DOIM
- Destruction
 - RAM, ROM, DRAM, SRAM, PROM Smart Cards, PDA's, and other electronic devices, etc.) - DOIM
 - DVD's & CD's - G2 (NSA/CSS evaluated and approved grinder, or completely destroy)
- Must be protected until destroyed!
- Use End-of-Day checks and Customizable Form 701 to check areas for classified before leaving for the day!

***** Use Spring Cleaning Concept (following Records Management Regs - destroy old and unused material).**

NOTE: Use DA Form 3964, Classified Document Accountability Record, to record the destruction of TS material.





Annual Security Training Industrial Shredder

Bldg T-679

0800 – 1530 hours

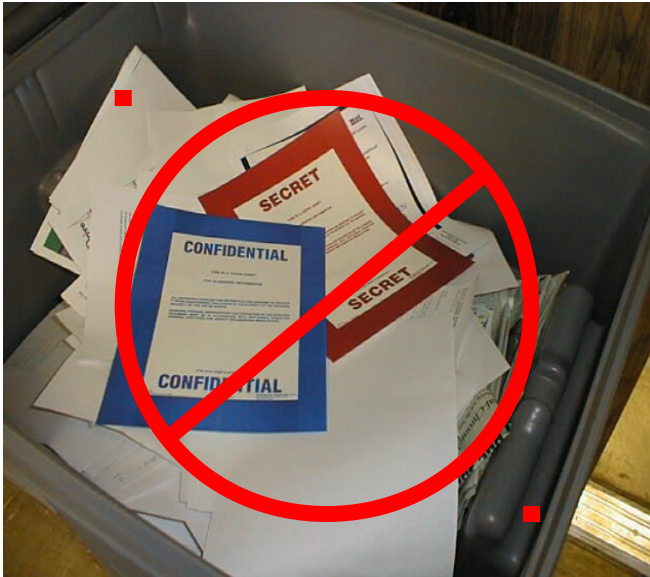
BY APPOINTMENT ONLY

Call 772-5003





Annual Security Training





Annual Security Training

Protecting Classified at Work

Emergency Evacuation and Destruction Plan

- A plan that provides for the Protection, Removal or Destruction of Classified Material in case of Fire, Natural Disaster, Civil Disturbance, Terrorist Activities or Enemy Action.
 - Detailed procedures / responsibilities for the protection of classified material.
 - Specific persons / positions.
 - Minimizes injury or loss of life
 - Allow senior person to deviate from the plan when necessary.
- Assign priorities based on damage to the US
 - Priority 1 (TS) - Exceptionally grave damage
 - Priority 2 (S) - Serious damage
 - Priority 3 (C) - Damage
 - Priority Markings are affixed to the interior of the safe drawers...
- When required, record the destruction of classified material.



Annual Security Training



End of Day Security Checks

- Check all areas to include safes, windows, desktops for classified
- Complete the SF 702, Security Container Checklist
- Complete the SF 701, Activity Security Checklist
- Turn on alarms if appropriate
- Lock doors

Fill in your own entries

| ACTIVITY SECURITY CHECKLIST | | DIVISION/BRANCH/OFFICE | | ROOM NUMBER | | MONTH AND YEAR | | | | | | | | | | | | | | | | | | | | | | | | | | |
|--|---|---|---|--------------------------|---|----------------|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|--|
| Irregularities discovered will be promptly reported to the designated Security Office for corrective action. | | Statement: I have conducted a security inspection of this work area and checked all the items listed below. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| FOUO (if required) | | FOUO (if required) | | Telephones (if required) | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ITEM | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | |
| 1. Security containers have been locked and checked. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 2. Desks, workstations and other surfaces and receptacles are free of classified material. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 3. Windows and doors have been locked (where appropriate). | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 4. Typewriter ribbons and ACP devices (e.g., files, name computers) classified material have been removed and properly stored. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 5. Security alarms and equipment have been activated (where appropriate). | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| INITIAL FOR DAILY REPORT | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| TIME | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 7501-101 NSA 7540-01-212-7089 | | STANDARD FORM 701 (Rev. 11-81) Approved by NSAS/SSO 12 APR 2003 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |



Annual Security Training

Protecting Classified at Work

Physical Security

- Perimeter Fences
- Employee and Visitor Access Controls
- Badges / Common Access Cards
- Intrusion Detection Systems
- Random Guard Patrols
- Prohibited Item Controls
- Entry / Exit Inspections
- Escorting
- Closed Circuit Video Monitoring



Annual Security Training

Operations Security (OPSEC)

OBJECTIVE: Conceal capabilities and intentions of tactical to strategic operations (G3 & DPTMS OPSEC Officer responsibility)

Four Major COMPONENTS (How to do):

- Physical Security (fences, guards, access control, etc)
- Information Security (marking, handling, transmission, storage and destruction)
- Signal Security (encryption and signal strength)
- Deception / Counter-Surveillance

Protect from the Foreign Intelligence Threat

- Human Intelligence
- Signals Intelligence
- Electronic Warfare
- Intelligence





Annual Security Training

Public release of
Government
information must first be
approved by the Public
Affairs
Office.





Annual Security Training

What Happens If...

- Security container is found open and unattended?
- Classified information is found unattended?
- Uncleared or unauthorized persons have accessed classified information?
- Other possible/actual compromise of classified information?

Report It!!!

Anyone who has knowledge of a security violation has a legal and moral obligation to report it.



Annual Security Training

Preliminary Inquiry

- Procedures are outlined in AR 380-5, chapter 10; not a full blown formal investigation.
- Designed to determine if a loss or compromise of classified material occurred.
- Also addresses possible systemic/procedural problems and/or weaknesses.

Inquiry Officer

- Appointed in writing by Commander or Staff Officer in the rank of LTC or higher (Authority is Para 2-1, AR 15-6).
- Rank/Grade:
 - **Military: SFC or higher**
 - **Civilian: GS07 or higher**
- Must be a disinterested party (not in the rating chain or chain of command).
- Must be equal to or senior to the individual(s) involved in the incident.
- Must have or be given sufficient time to conduct inquiry.
- Must be cleared at the same or higher level of classified material involved in the incident.



Annual Security Training

Appointing Authority

Inquiry Officer provides Written Report to the Appointing Authority within 20 working days* of the incident.

- Is further investigation needed?
- Is there evidence or indications of willful intent to compromise classified material?
- Was this caused by an individual(s) and is disciplinary/administrative action warranted?
- What is recommended to correct systemic flaws and weaknesses?

Review with recommendations from Appointing Authority, through the chain-of-command, to the Division or Installation Security Manager within three working days*.

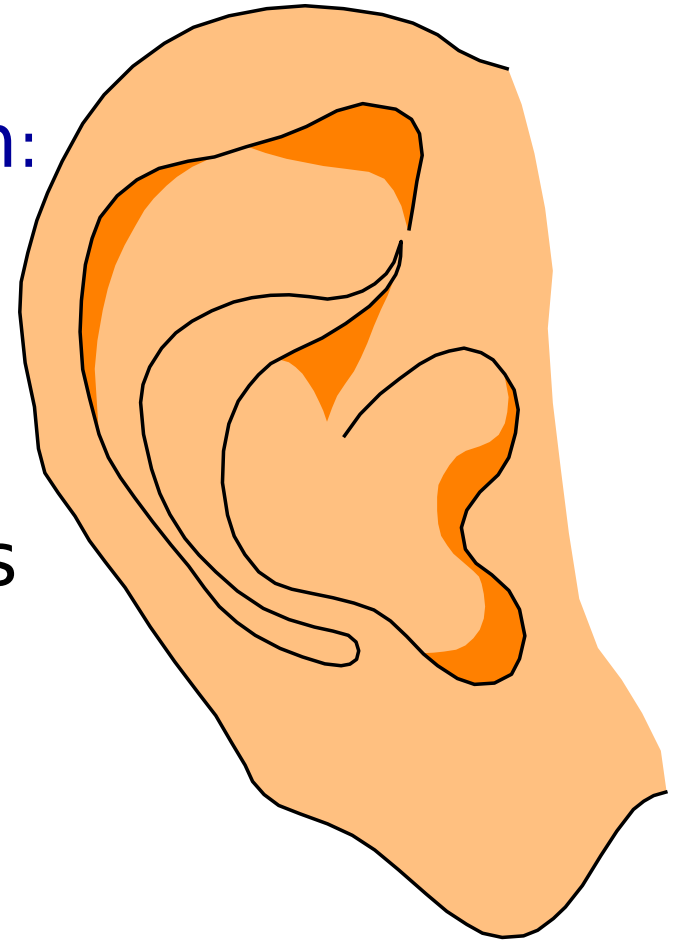
* Reference: FORSCOM Supplement 1 to AR 380-5



Annual Security Training

Most leaks result from:

Negligence
Carelessness
Casual Conversations





Annual Security Training

Inspections

AR380-5 & FORSCOM Suppl 1 to AR380-5: Subordinate Units “No less than once every other year”

Fort Drum Reg 1-3: Fort Drum Command Inspection Program

- Appendix I – 01 (Information Security)
- Appendix I – 02 (Personnel Security)
- Appendix I – 03 (Antiterrorism)
- Appendix J – (Intelligence Oversight)



Annual Security Training

Questions?





Annual Security Training

WHY SECURITY?

- DoD Security Regulation, Directives and Programs are established to counter threats.
- Threats to classified and unclassified government assets includes:
 - Insider (e.g., government employees, contractor employees and authorized visitors).
 - Criminal and Terrorist Activities.
 - Foreign Intelligence Services.
 - Foreign Governments.



Annual Security Training

Subversion and Espionage Directed Against the US Army (SAEDA)

- US Army - A Prime Target
- Situations to report:
 - Attempts to obtain information (while at Fort Drum, at home, or while traveling)
 - Intimidation while traveling through foreign countries
 - Exploitation of another person
 - Act or attempt to compromise classified
 - Known or suspected deliberate compromise

NOTE 902nd MI Responsibility



Annual Security Training

TRADITIONAL THREAT

N. KOREA



RUSSIA



CHINA



Iran

Cuba

Iraq

Argentina

Afghanistan

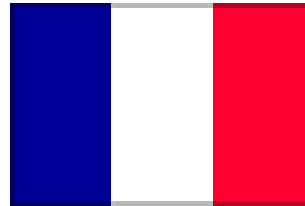
Syria



Annual Security Training

NON-TRADITIONAL THREAT

FRANCE



KOREA



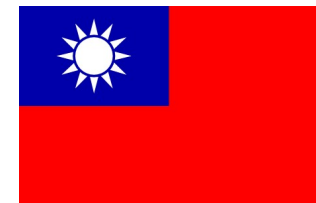
ISRAEL



INDIA



TAIWAN





Annual Security Training

**Montreal and Quebec, Canada, and
Vancouver, British Columbia**
• Al-Qaeda

**Lackawanna and
Syracuse, NY**
• Al-Qaeda
Webster, NY
• Jamaat Al-Fuqua
Rochester, NY
• Al-Qaeda

Jersey City/Paterson, NJ
• Gamat Islamiyah
Newark, NJ
• Al-Qaeda

Philadelphia, PA
• Al-Muhajirum
• Gamat Islamiyah
• HAMAS
• Hizballah

Cleveland, OH
• Al-Qaeda

Springfield/Herndon, WV
• HAMAS
• AQ

Hancock, NY
• Jamaat Al-Fuqua

Ottawa and Toronto, Canada
• Hezbollah
• Hamas (Ottawa only)
• Al-Qaeda

Berrysbay, Canada
• Jamaat Al-Fuqua

Boston, MA
• Gamat Islamiyah
• National Islamic Front

New York City
• Al-Muhajirum
• Gamat Islamiyah
• HAMAS
• Hizballah
• Al-Qaeda
• Tamil Tigers
• "Domestic"-Herald Square Subway
• "Domestic"-The Al Muhajiroun Towers

FT Dix, NJ
• "Domestic Terrorist" Cell-Pizza Delivery

Baltimore, MD
• Gamat Islamiyah

Washington DC
• Gamat Islamiyah
• HAMAS
• Hizballah



Annual Security Training

Subversion: Advocating or causing insubordination, disloyalty, mutiny, or refusal of duty by any DOD personnel with the intent to impair the loyalty, morale, discipline or mission of the U.S. Armed Forces.

Espionage: The act of obtaining, delivering, transmitting, or communicating National Defense information with the intent or reason to believe it may be used to injure the U.S. or give an advantage to a foreign nation.

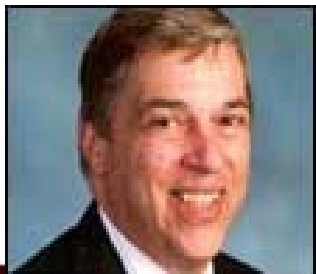




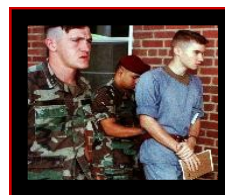
Annual Security Training



Indicators of Espionage



- Attempts to expand classified access
- Unauthorized removal of classified
- Extensive reproduction / transmission of classified
- Work outside normal duty hours
- Tries to get witness signature--without seeing destruction
- Unauthorized devices around classified
- Unexplained affluence (\$)
- Money with no logical source
- Free spending / lavish display of wealth
- Sudden reversal of financial condition
- Correspondence/Business dealings from foreign countries
- Contact with ANY Foreign Intelligence Service (FIS) or foreign officials
- Frequent foreign trips
- Offer extra income to those with sensitive jobs
- Homesteading undesirable jobs
- Repeated security violations
- Joking / bragging about working for foreign intelligence





Annual Security Training

Title 50, USC, Sec. 783 War & National Defense

Unauthorized Disclosure of Classified Information. It is unlawful to give classified information to an agent or representative of any foreign government that would result in harm to the National Security.





Annual Security Training

Title 18, USC, Sec. 794 Crimes & Criminal Procedures

- Sec. 794. Gathering or delivering defense information to aid of foreign government
- Delivery of defense information with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign nation, shall be punished by death or by imprisonment for any term of years or for life...,



Annual Security Training

Title 18, USC, Sec. 798

- (1) Any person convicted of a violation of this section shall forfeit to the United States irrespective of any provision of State law -
- (A) any property constituting, or derived from, any proceeds the person obtained, directly or indirectly, as the result of such violation; and
(B) any of the person's property used, or intended to be used, in any manner or part, to commit, or to facilitate the commission of, such violation.





Annual Security Training

What Do You Report?

Through the Chain-of-command:

- Loss, compromise, or suspected compromise of classified information or material - Investigate IAW AR380-5, chapter 10
- Security violations - Investigate IAW AR380-5, chapter 10
- Adverse Information (e.g., medical conditions, UCMJ, administrative or law enforcement issues, etc.) - JPAS (CDR determines continued access)
- Change in individuals' status (e.g., PCS, ETS, etc.) - JPAS changes / SID
- Questionable or suspicious contacts (e.g., requests classified information, wants more information than they need to know, and acts suspiciously) - 902nd?
- All cleared employees must report contact with foreign nationals



Annual Security Training

Espionage, Sabotage or Subversive Activities are Reported To Whom?

- ✓ 902d Military Intelligence Group
- ✓ G-2, 10th MTN Div
- ✓ Security and Intelligence Division
- ✓ 1 - 800 - CALLSPY

DO NOT tell the whole Chain of Command!
DO NOT take any action YOURSELF.



Annual Security Training

Penalties for Compromising Classified Material

- Access denied
- Suspended security clearance (employment ramifications)
- Reprimand or other Administrative penalties
- Suspension
- Other actions in accordance with the UCMJ, or laws and regulations



Annual Security Training

Who is responsible for security?

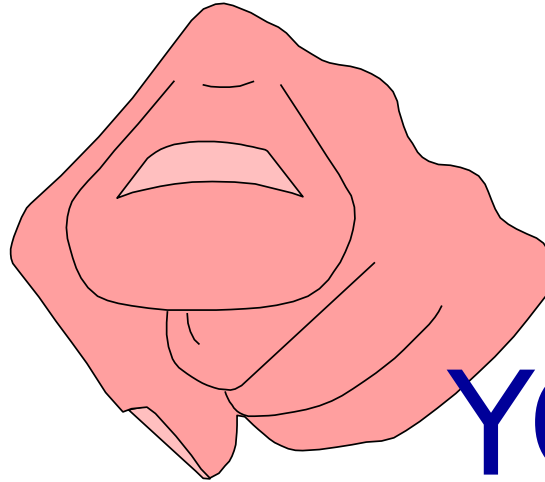


© Scott Adams, Inc./Dist. by UFS, Inc.



Annual Security Training

YOU!



YOU!



YOU!